ITRI 625

Pfleeger Chapter 6

Whitman & Mattord Chapters 6 & 7

Environment of use

- The biggest difference between a network and a stand-alone device is the environment in which each operates.

- Networks can be described by several typical characteristics:

  - Anonymity. A network removes most of the clues by which we recognize acquaintances.
  - Automation. In some networks most points involved might be machines with only minimal human supervision.
  - Distance. Networks connect endpoints with such speed that users typically cant tell whether a remote site is near or far.
  - Opaqueness. Users cannot distinguish where the node they are connected to is located. They cant even tell if they are communicating with the same host than the previous time.
  - Routing diversity. The same interaction might follow different paths each time it is invoked.

What makes a network vulnerable?

- Anonymity. An attack can be mounted without ever coming into contact with the system, its administrators, or users.
- Many points of attack – both targets and origins. An attack can come from any host to any host, therefore many points of vulnerability.
- Sharing. Access is afforded to more users and systems. Access controls for single systems may be inadequate in networks.
- Complexity of system. A network OS is more complex than an OS for a single computing system. This inherent complexity makes it extremely difficult, if not impossible, to secure.
- Unknown perimeter. A network's expandability also implies uncertainty about the network boundary.
- Unknown path. There are many paths from one host to another. Network users seldom have control over the routing of their messages.

Main types of attacks

- Reconnaissance. For example port scans, for intelligence, for social engineering, etc.
- Threats in transit: Eavesdropping and Wiretapping. These types of threats can occur across all transmission media.
- Impersonation. For example authentication foiled by guessing, nonexistent authentication, masquerade, etc.
- Message confidentiality threats. For example misdelivery (although uncommon), exposure, traffic flow analysis, etc.
- Message integrity threats. For example falsification of messages and noise.

Main types of attacks *cont.*

- Format failures. For example malformed packets, protocol failures and implementation flaws.
- Web site vulnerabilities. For example web site defacement, application code errors, etc.
- Denial of service. For example transmission failure, connection flooding, traffic redirection, etc.
- Threats in active or mobile code. For example cookies, scripts, etc.
- Complex attacks. For example script attacks and building blocks.

Network security controls

- Architecture. Planning can be the strongest control, especially when planning to build in security as one of the key constructs.
    - Segmentation. Segmentation reduces the number of threats, and it limits the amount of damage a single vulnerability can allow.
    - Redundancy. Allowing a function to be performed on more than one node, to avoid "putting all your eggs in one basket".
    - Single points of failure. Is there a single point in the network that if it were to fail, could deny access to all or a significant part of the network?
    - Mobile agents. Mobile code and hostile agents are potential methods of attack, but they can also be forces for good.

Network security controls *cont.*

- Encryption. Encryption is probably the most important and versatile tool for a network security expert.
  - Link encryption. Data are encrypted just before the system places them on the physical communications link.
  - End-to-end encryption. Provides security from one end of a transmission to the other.
  - SSH encryption. Provides an authenticated and encrypted path to the shell or operating system command interpreter.
  - SSL encryption. SSL interfaces between applications and the TCP/IP protocols to provide server authentication, optional client authentication, and an encrypted communications channel between client and server.

Network security controls *cont.*

- Strong authentication. Authentication may be more difficult to achieve securely because of the possibility of eavesdropping and wiretapping.
  - One-time password. Good for one use only.
  - Challenge-response systems. A more sophisticated one-time password scheme. Uses a device that functions as an intermediary for authentication.
  - Digital distributed authentication. Developed due to the need to authenticate nonhuman entities in a computing system.
  - Kerberos. Used for authentication between intelligent processes, such as client-to-server tasks, or a user's workstation to other hosts (see p. 461). Supports authentication in distributed systems.

Network security controls *cont.*

- Wireless security. Being so exposed, it requires special measures to protect communication.
  - SSID. The service set identifier is the identification of an access point.
  - WEP. Meant to provide users privacy equivalent to that of a dedicated wire.
  - WPA and WPA2. Addresses the security deficiencies known in WEP.
  - Alarms and alerts. Devices that are placed inside protected networks to monitor what occurs inside the networks.
  - Honeypots. Computer systems open to attackers with the ideal of catching them.

Firewalls

- A firewall is a device that filters all traffic between a protected or "inside" network and a less trustworthy or "outside" network. Its purpose is to keep "bad" things outside a protected environment.

- Types of firewalls include:

1. Packet filtering gateways. The simplest type of firewall that controls access to packets on the basis of packet address or specific transport protocol type.

2. Stateful inspection firewalls. An improvement through maintaining state information from one packet to another in the input stream.

Firewalls *cont.*

3. Application proxies. A firewall that simulates the proper effects of an application so that the application receives only requests to act properly.

4. Circuit gateway. A firewall that essentially allows one network to be an extension of another

5. Guards. A sophisticated firewall that decides what services to perform on the user's behalf in accordance with its available knowledge, such as whatever it can reliably know of the outside user's identity, previous interactions, and so forth.

6. Personal firewalls. An application program that runs on a workstation to block unwanted traffic, usually from the network. Complements the work of a conventional firewall.

See table 6.6 on page 468 for a summary.

Intrusion detection systems

- A device, typically another separate computer, that monitors activity to identify malicious or suspicious events.

- Types of IDSs:

  - Signature based. Performs simple pattern matching and reports situations that match a pattern corresponding to a known attack type.

  - Heuristic based. Build a model of acceptable behavior and flag exceptions to that model.

  - Network based. A standalone device attached to the network to monitor traffic throughout that network.

  - Host based. Runs on a single workstation or client or host, to protect that one host.

Goals for IDSs

- An IDS should be fast, simple, and accurate, while at the same time being complete.

- An IDS could use some or all of the following design approaches:
  - Filter on packet headers.
  - Filter on packet content.
  - Maintain connection state.
  - Use complex, multipacket signatures.
  - Use minimal number of signatures with maximum effect.
  - Filter in real time, online.
  - Hide its presence.
  - Use optimal sliding time window size to match signatures.

Security for e-mail

- Threats to e-mails include:
  - Message interception (confidentiality).
  - Message interception (blocked delivery).
  - Message interception and subsequent replay.
  - Message content modification.
  - Message origin modification.
  - Message content forgery by outsider.
  - Message origin forgery by outsider.
  - Message content forgery by recipient.
  - Message origin forgery by recipient.
  - Denial of message transmission.

Security for e-mail *cont.*

- The requirements for secure e-mail include:

1. Message confidentiality.
2. Message integrity.
3. Sender authenticity.
4. Nonrepudiation.

- Encryption can be used to address all the requirements identified above. Not only the message is encrypted, but all the header information as well. A message integrity check can also be incorporated to further ensure integrity.

- Key management is however the major problem with e-mail encryption.

Questions

- Any questions?

ITRI 625

Pfleeger Chapter 7

Database security requirements

- **Physical database integrity**. The data in a database should be immune to physical problems, such as power failures. Someone should be able to reconstruct it if it is destroyed in a catastrophe.

- **Logical database integrity**. The structure of the database should be preserved. For example a modification in one field should not affect the other fields.

- **Element integrity**. The data contained in each element should be accurate. Can be ensured in three ways:

1. Field checks, where data type and format is checked.
2. Access control, where only certain people can make modifications.
3. Change log, where a log is kept of all changes made, thereby simplifying corrections.

Security requirements *cont.*

- **Auditability**. A record that is kept of all accesses that were made to the database, thereby assisting with the database's integrity.

- **Access control**. The database administrator specifies who should be allowed access to which data, at the view, relation, field, record or even element level.

- **User authentication**. The DBMS usually performs its own authentication, which in turn improves security and integrity.

- **Availability.** The DBMS tends to be taken for granted, and quite often "unavailability" is merely the system servicing another user.

Update integrity

- A system failure in the middle of modifying data is a serious problem (see page 514).

- The two-phase update has been developed to address this problem.

1. The intent phase. The DBMS gathers the resources it needs to complete the update, it prepares everything, but makes no changes. It is a repeatable phase and therefore no harm is done if a system failure occurs during this phase. The last event is committing, during which a commit flag is written. After committing the DBMS starts making permanent changes.

2. Also a repeatable phase during which the changes are made. If a failure occurs, the system can repair it by repeating the phase. Once this phase is complete, the database is complete.

Inference

- A way to infer or derive sensitive data from non-sensitive data.
- Direct attacks. Where users try to determine values of sensitive fields by seeking them directly with queries that yield few records.
- Indirect attacks (see page 521). Seeks to infer a final result based on one or more intermediate statistical results. Only neutral data is released, identifying characteristics are removed.
- Tracker attacks (see page 524). A DBMS may conceal data when a small number of entries make up a large proportion of the data revealed. These attacks fool the manager into locating the desired data by using additional queries that produce small results.

Inference *cont.*

- Linear system vulnerability (see page 525). With a little logic algebra, and luck in the distribution of the database contents, it may be possible to construct a series of queries that returns results relating to several different sets.

- See pages 529 – 535 for controls for inference attacks.

- There are no perfect solutions to the inference problem. The three main approaches to controlling it are:

1. Suppress obviously sensitive information.
2. Track what the user knows.
3. Disguise the data.

Multilevel databases

- Data cannot always only be classified as sensitive or non-sensitive.
- Three characteristics of database security that emerge are:

1. The security of a single element may be different from the security of other elements of the same record or from other values of the same attribute.
2. Two levels are inadequate to represent some security situations.
3. The security of an aggregate may differ from the security of the individual elements.

Proposals for multilevel security

- **Partitioning.** Where the database is divided into separate databases each at its own level of sensitivity. It does however destroy the advantage of elimination of redundancy and improved accuracy.
- **Encryption**. Each level of sensitive data can be stored in a table encrypted under a key unique to the level of sensitivity.
- **Integrity lock**. Provides both integrity and limited access. Each data item consists of three pieces. The actual data item itself, a sensitivity label and a checksum. The checksum is computed to prevent unauthorized modification.
- **Sensitivity lock.** A combination of a unique identifier and the sensitivity level. Because the identifier is unique, each lock relates to one particular record.

Security in data mining

- In a largely automated way, data mining applications sort and search through data.
- They present probable relationships, but these are not necessarily cause-and-effect relationships.
- **Privacy and sensitivity**. Although summarized results are used, individual privacy can still suffer. It suffers from the same kinds of aggregation and inference found in databases.
- **Data correctness and integrity.** Connecting the dots refers to drawing conclusions from relationships between discrete bits of data. The correct data should be collected correctly.

Security in data mining *cont.*

- **Correcting mistakes in data.** Quite often correcting a mistake requires a mistake to be rectified on a master record. In typical marketing scenarios this tends not to be the case. Data mining often takes place across databases that do not have shared keys, so they use data fields as keys. This typically leads to a mistake occurring in several places.

- **Using comparable data.** Data semantics is very important in data mining. When comparing fields in two different databases, they should be in the same format, to avoid badly distorted statistics.

- **Eliminating false matches.** Data mining will inevitably produce false positives and missed connections. We need to be sensitive to the inherent inaccuracy of data mining approaches. Correctness of results and interpretations are major security issues.

Questions

- Any questions?

ITRI 625

Pfleeger Chapter 9

Privacy concepts

- Privacy is the right to control who knows certain aspects about you, your communications, and your activities.

- Information privacy has three aspects, sensitive data, affected parties, and controlled disclosure.

1. Controlled disclosure. As soon as you give out your number for example, your control is diminished because it depends in part on what someone else does. You do not control the other person.

2. Sensitive data. Some examples of data many people consider private include, identity, finances, legal matters, religion, etc.

3. Affected subject. The entity involved governs the data and possible consequences.

Computer related privacy problems

- The eight dimensions of computer related privacy are:

1. Information collection. Only with knowledge and explicit consent.
2. Information usage. Only for certain specified purposes.
3. Information retention. Only for a set period of time.
4. Information disclosure. Only to authorized people.
5. Information security. Appropriate mechanisms are used to ensure protection.
6. Access control. All modes of access are controlled.
7. Monitoring. Logs are maintained showing all accesses.
8. Policy changes. Less restrictive policies are never applied after-the-fact to already obtained data.

Steps to protect against privacy loss

- Several steps that any entity can take to help safeguard private data include:

- Data minimization.
- Data anonymization.
- Audit trail.
- Security and controlled access.
- Training.
- Quality.
- Restricted usage.
- Data left in place.
- Policy.

Authentication and privacy

- Authentication can refer to authenticating an individual, identity, or attribute.
- An individual is an unique person. There are relatively few ways of identifying an individual, and usually weak authentication is acceptable.
- An identity is a character string or similar descriptor. From a privacy standpoint, there may or may not be ways to connect different identities. Depending on the application, it can typically be done through linking, especially when authentication is not ideal and anonymity is required.
- An attribute is a characteristic. By linking various characteristics, privacy can quite often be jeopardized. Research has indicated that the process of effectively anonymizing data is extremely difficult.

Privacy on the web

- The internet is perhaps the greatest threat to privacy.
- It is like a nightmare of a big, unregulated bazaar, where every word you speak can be heard by many others.
- Payments on the web are perhaps one of the main privacy concerns, and nowadays mainly credit cards or payment schemes are used for online transactions.
- Sites and portals often require registering before being able to use their services. More often than not this information is used for marketing or to show that advertisements are warranted.
- Third party ads, contests and offers are great ways for companies to collect information and draw links.

Privacy on the web *cont.*

- Precautions for web surfing include limiting cookies and web bugs, two technologies that are frequently used to monitor a user's activities without the user's knowledge.
- Cookies are files of data sent by a website, and are a cheap way of transferring storage needs from a website to a user.
- Third party cookies are for organizations other than the webpage's owner.
- A cookie is a tracking device, whereas a web bug is an invisible image that invites or invokes a process. The image is typically 1 x 1 pixel, so virtually invisible on modern resolutions.

Privacy on the web *cont.*

- Spyware code is designed to spy on a user to obtain information.
- Keystroke loggers, the computer equivalent of a telephone wiretap.
- Hijackers, software that hijacks a program installed for a different purpose.
- Adware, displays selected ads in pop-up windows with the aim of obtaining personal information.
- Drive-by installation, a means of tricking a user into installing software. It conceals from the user the real code being installed.

Impacts on emerging technologies

- Applications of three emerging technologies have inherent risks for privacy.

1. Radio frequency identification (RFID). Small, low power wireless radio transmitters. When a tag receives a signal it sends its ID number in response. Its major concerns are the ability to track people wherever, and correctness.

2. Electronic voting. Ensuring anonymity whilst voting using computers is extremely difficult. Both in capturing the vote and in transmitting it to the election headquarters.

3. Voice over IP (VoIP). Even if solidly encrypted, the source and destination of the phone call will be somewhat exposed through packet headers.

4. Internet of Things (IoT). Insecure products can lead to potentially catastrophic consequences.

Questions

- Any Questions?

ITRI 625

Pfleeger Chapter 10

Whitman & Mattord Chapters 4 & 5

Security planning

- A good security plan is an official record of current security practices, plus a blueprint for orderly change to improve those practices.

- Every security plan must address seven issues.

1. Policy.
2. Current state.
3. Requirements.
4. Recommended controls.
5. Accountability.
6. Timetable.
7. Continuing attention.

Security planning *cont.*

- A security planning team should represent each of the following groups:

1. Computer hardware group.
2. System administrators.
3. Systems programmers.
4. Applications programmers.
5. Data entry personnel.
6. Physical security personnel.
7. Representative users.

- Three groups of people must contribute to make the plan a success.

1. The planning team being sensitive to the needs of each group.
2. Those affected must understand the plan's implications.
3. Management being committed to using and enforcing the plan.

Risk analysis

- A risk is a potential problem that the system or its users may experience.

- We distinguish a risk from other project events by looking for three things:

1. A loss associated with an event.
2. The likelihood that the event will occur.
3. The degree to which we can change the outcome.

- The three strategies for dealing with risk are:

1. Avoiding the risk.
2. Transferring the risk.
3. Assuming the risk.

Risk analysis *cont.*

- Risk analysis is the process of examining a system and its operational context to determine possible exposures and the potential harm they can cause.

- The basic steps of a risk analysis are:

1. Identify assets.
2. Determine vulnerabilities.
3. Estimate likelihood of exploitation.
4. Compute expected annual loss.
5. Survey applicable controls and their costs.
6. Project annual savings of control.

Risk analysis *cont.*

- There are many good reasons to perform a risk analysis in preparation for creating a security plan.

1. Improve awareness.
2. Relate security mission to management objectives.
3. Identify assets, vulnerabilities and controls.
4. Improve basis for decisions.
5. Justify expenditures for security.

- However, despite the advantages there are also several arguments against it.

1. False sense of precision and confidence.
2. Hard to perform.
3. Immutability.
4. Lack of accuracy.

Organizational security policies

- A security policy is a high-level management document to inform all users of the goals of and constraints on using a system.

- They are used for several purposes, including:

1. Recognizing sensitive information assets.
2. Clarifying security responsibilities.
3. Promoting awareness for existing employees.
4. Guiding new employees.

- A security policy addresses several different audiences with different expectations. Each group uses the security policy in important but different ways.

Organizational security policies *cont.*

- A security policy must identify its audiences and describe the nature of each audience and their security goals.
- The policy should state the purpose of the organization's security functions, reflecting the requirements of beneficiaries, users and owners.
- A security policy must be comprehensive, and if it is written poorly, it cannot guide the developers and users in providing appropriate security mechanisms to protect important assets.
- A security policy must grow and adapt well, as an obscure or incomplete policy will not be implemented properly, if at all.

Physical security

- As discussed in ITRI615, physical security is the term used to describe protection needed outside the computer system.

- Many physical security measures can be provided simply by good common sense.

- With regards to physical security from an administration perspective, the following need to be considered:
  - Natural disasters.
  - Power loss.
  - Surge suppressor.
  - Human vandals.
  - Interception of sensitive information.
  - Contingency planning. The key to successful recovery is adequate planning.

Questions

- Any Questions?

ITRI 625

Pfleeger Chapter 11

Legal and ethical issues in computer security

- There are three motivations for studying the legal aspects of computer security:

1. To know what protection the law provides for computers and data.

2. To appreciate laws that protect the rights of others with respect to computers, programs and data.

3. To understand existing laws as a basis for recommending new laws to protect computers, data, and people.

We need to protect computing systems against criminals, code and data, programmers' and employers' rights, and users of programs.

Protecting programs and data

- Copyrights. First step is notice, then filing at the copyrights office.
- Intellectual property.
- Originality of work.
- Fair use of material.
- Copyrights for digital objects. The Digital Millennium Copyright Act (or DMCA) came into effect in 1998.
- Patents. Obtained by convincing the patent office that an invention deserves a patent. Not encouraged for computer software.

Protecting programs and data *cont.*

- Trade secrets. Information that gives one company a competitive edge over others.
- Can be discovered through reverse engineering. Start with the finished product and work backwards.
- Extremely applicable to computer objects as it allows distribution of the result of a secret while still keeping the program design hidden.
- See table 11.1 on page 716 for a summary.

Rights of employees and employers

- The age old question of who owns a product?
- Patent ownership is based on who files the patent application.
- In general with copyrights the creator is considered to be the owner of the work.
- In a work for hire situation the employer is considered the author of a work. The employer is seen as coming up with the idea.
- Licenses. With licenses the programmer is considered the author, which then provides license for companies to use the work.
- Employment contracts often spell out rights of ownership.

Computer crime

- Rules of property. The legal system has explicit rules about what constitutes property.
- Rules of evidence. The biggest difficulty with computer based evidence in court is being able to demonstrate the authenticity of the evidence.
- Threats to integrity and confidentiality. The integrity and secrecy of data are also issues in many court cases.
- Value of data. How much is data that has been stolen really worth?
- Acceptance of computer terminology. The law is lagging behind technology in its acceptance of definitions of computing

  terms.

Computer crime *cont.*

- Computer crime is hard to prosecute for the following reasons:

1. Lack of understanding.
2. Lack of physical evidence.
3. Lack of recognition of assets.
4. Lack of political impact.
5. Complexity of case.
6. Age of defendant.

Ethical issues in computer security

- It is impossible or impractical to develop laws to describe and enforce all forms of behavior acceptable to society. Society tends to rely on ethics to prescribe generally accepted standards of proper behavior.

- An ethic is an objectively defined standard of right and wrong. A set of ethical principles is called an ethical system.

- See table 11.3 on page 745 for a contrast of law vs. ethics.

- Ethics and religion. Although they might influence one another, the one does not determine the other.
- Ethical principles are not universal. Ethical values vary by society, and from person to person within a society.

Ethical issues in computer security *cont.*

- Ethics does not provide answers. Ethical pluralism is recognizing or admitting that more than one position may be ethically justifiable in a given situation.
- See table 11.4 on page 750 for a taxonomy of ethical theories.
- Also see section 11.7 for case studies of ethics.
- Because of such ethical issues, various computer groups have sought to develop codes of ethics for their members. Among these are the IEEE, ACM, and the computer ethics institute.

Questions

- Any Questions?

ITRI 625

Pfleeger Chapter 13

Making a business case

- Various internal and external pressures drive organizations to scrutinize the amount and effectiveness of their cyber security practices and products.

- Any evaluation of an existing or proposed investment in technology should be reported in several ways at once to form a "balanced scorecard".
  - From a customer view, addressing issues such as customer satisfaction
  - From an operational view, looking at organizational core competencies
  - From a financial view, measures such as ROI or share price
  - From an improvement view, how the investment will affect market leadership and added value

Determining economic value

- Economic value can be a unifying principle in considering any business opportunity. There are many different ways to capture it, including:

1. Net present value. The present value of the benefits minus the value of the initial investment.
2. Internal rate of return. Derived from the NPV and is equal to the discount rate that makes the NPV equal to zero.
3. Return on investment. Generated by dividing the last period's accounting profits by the cost of the investments required to generate those profits.

- In general, businesses need to know whether and how investing one more unit buys them more security.

Modeling cyber security

- Cyber security economics brings together elements of cyber security and economics to help decision makers to invest already constrained resources.

- Among the many questions asked about cyber security investments are:

1. How much should an organization invest in cyber security to protect assets of a given value? Can be addressed by applying accounting techniques to develop a model of information protection.
2. What is the likely impact of a security breach? Can be addressed by examining the economic effect of information security breaches reported in newspapers and publicly traded corporations.
3. What are the costs and benefits of sharing information? Addressed using game theory. Two competing organizations are pitted against each other to obtain models of cost and demand.

Modeling cyber security *cont.*

- When presented with information about risk in terms of probability and payoff, researchers have found that:

1. When the payoff is small, people focus on the risk.
2. When the risk is small, people focus on the payoff.

- Many cyber security risks have a very small likelihood of occurrence but can have an enormous impact in terms of cost, schedule, inconvenience, or even human life.

- Group behavior dynamics has also been widely researched, and it has been documented how group dynamics can influence decision-making. It extends beyond teams to affect clients, colleagues and even competitors.

The role of organizational culture

- Trust and interpersonal relations are solidly linked to economic behavior. The typical dimensions of organizational culture are:

Pole 1	Pole 2	Explanation
Process oriented	Results oriented	Means vs. goals
Employee oriented	Job oriented	Concern for people vs. completing job
Parochial	Professional	Identity from organization vs. profession
Open system	Closed system	With respect to newcomers
Loose control	Tight control	With respect to employee autonomy
Normative	Pragmatic	Rule-based vs. job-driven

The role of organizational culture *cont.*

- Organizations seldom fall into a specific dimension, and tend to lie somewhere in the middle, between dimensions.

- These dimensions affect an organization's cyber security economics.

- The organizational culture reflects the underlying organizational values and therefore suggests the kinds of choices likely for cyber security investment behavior. For example:
  - A results-driven organization may choose to invest in penetrate-and-patch behavior rather than in best-practice training.
  - A professional organization may certify all its security professionals, but a parochial one may prefer to invest instead in rewarding those developers whose products have the fewest security failures after release.

Questions

- Any Questions?